0038·0431PUS1
NEW
April 15, 2004
Yuji HANDA et al.
BSKB
703·205·8000

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月２２日

出願番号
Application Number: 特願２００３－１１７３８３

[ST. 10/C]: [ＪＰ２００３－１１７３８３]

出願人
Applicant(s): シナノケンシ株式会社

２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００５７５８

【書類名】　特許願

【整理番号】　P0354128

【提出日】　平成15年 4月22日

【あて先】　特許庁長官　　殿

【国際特許分類】　G06F 12/14

G09C 1/00

【発明の名称】　データ書き込み方法およびデータ読み込み方法と、これらを用いたデータ記録装置

【請求項の数】　14

【発明者】

【住所又は居所】　長野県上田市中央６－１５－２６　シナノケンシ株式会社　電子機器事業部内

【氏名】　半田　雄士

【発明者】

【住所又は居所】　長野県上田市中央６－１５－２６　シナノケンシ株式会社　電子機器事業部内

【氏名】　高橋　和樹

【特許出願人】

【識別番号】　000106944

【氏名又は名称】　シナノケンシ株式会社

【代理人】

【識別番号】　100077621

【弁理士】

【氏名又は名称】　綿貫　隆夫

【選任した代理人】

【識別番号】　100092819

【弁理士】

【氏名又は名称】　堀米　和春

【手数料の表示】

【予納台帳番号】　006725

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9702285

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　データ書き込み方法およびデータ読み込み方法と、これらを用いたデータ記録装置

【特許請求の範囲】

【請求項１】　記憶手段と、

記録媒体にデータを書き込むデータ書き込み手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化手段とにより構成されるデータ記録装置におけるデータ書き込み方法であって、

前記書込み手段が、外部機器に設けられたライトアプリケーションにより構築された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させるステップと、

前記暗号化手段が、ユーザにより設定され、かつ、入力されたパスワードに基づいて前記記録媒体の認識時に使用されるシステム領域データの一部又は全てを所定のアルゴリズムで暗号化するステップと、

前記記憶手段に前記データを記憶させるステップと、

前記データ書込み手段が、該暗号化した記録媒体の認識時に使用されるシステム領域データを前記記録媒体の所定領域に書き込むステップと、

前記データ書き込み手段が、前記データを前記記録媒体に書き込むステップとを有することを特徴とするデータ書き込み方法。

【請求項２】　記憶手段と、

記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段とにより構成されるデータ記録装置におけるデータ読み込み方法であって、

前記読み込み手段が、前記記録媒体の所定領域に格納されている記録媒体の認識時に使用されるシステム領域データにアクセスすると共に、暗号化された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させるステップと、

前記復号化手段が、ユーザにより設定され、かつ、入力されたパスワードに基づいて、所定のアルゴリズムにより前記記録媒体の認識時に使用されるシステム領域データを復号化するステップとを有することを特徴とするデータ読み込み方法。

【請求項３】　記憶手段と、

記録媒体にデータを書き込むデータ書き込み手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化手段と、

各手段の動作を制御する制御手段とにより構成され、

データ書き込み時において、前記制御手段が、

前記書込み手段に、外部機器に設けられたライトアプリケーションにより構築された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、

前記暗号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて前記記録媒体の認識時に使用されるシステム領域データの一部又は全てを所定のアルゴリズムで暗号化させ、

前記記憶手段に前記データを記憶させ、

前記データ書込み手段に、該暗号化した記録媒体の認識時に使用されるシステム領域データを前記記録媒体の所定領域に書き込ませ、

前記データ書き込み手段に、前記データを前記記録媒体に書き込ませる処理を実行することを特徴とするデータ記録装置。

【請求項４】　記憶手段と、

記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、

各手段の動作を制御する制御手段とにより構成され、

データ読み込み時において、前記制御手段が、

前記読み込み手段に、前記記録媒体の所定領域に格納されている記録媒体の認識時に使用されるシステム領域データにアクセスさせると共に、暗号化された記録

媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、

前記復号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて、所定のアルゴリズムにより前記暗号化された記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することを特徴とするデータ記録装置。

【請求項５】　記憶手段と、

記録媒体にデータを書き込むデータ書き込み手段と、

記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化手段と、

ユーザにより設定され、かつ、入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、

各手段の動作を制御する制御手段とにより構成され、

データ書き込み時において、前記制御手段が、

前記書込み手段に、外部機器に設けられたライトアプリケーションにより構築された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、

前記暗号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて前記記録媒体の認識時に使用されるシステム領域データの一部又は全てを所定のアルゴリズムで暗号化させ、

前記記憶手段に前記データを記憶させ、

前記データ書込み手段に、該暗号化した記録媒体の認識時に使用されるシステム領域データを前記記録媒体の所定領域に書き込ませ、

前記データ書き込み手段に、前記データを前記記録媒体に書き込ませる処理を実行し、

データ読み込み時において、前記制御手段が、

前記読み込み手段に、前記記録媒体の所定領域に格納されている記録媒体の認識時に使用されるシステム領域データにアクセスさせると共に、暗号化された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、

前記復号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて、所定のアルゴリズムにより前記記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することを特徴とするデータ記録装置。

【請求項６】　前記記憶手段には、補助パスワードがあらかじめ記憶されていて、

前記制御手段は、ユーザにより設定され、かつ、入力されたパスワードに、前記補助パスワードを付加した後に、前記暗号化手段に前記記録媒体の認識時に使用されるシステム領域データを暗号化させる処理を実行することを特徴とする請求項３または５に記載のデータ記録装置。

【請求項７】　前記記憶手段には、補助パスワードがあらかじめ記憶されていて、

前記制御手段は、ユーザにより設定され、かつ、入力されたパスワードに前記補助パスワードを付加した後に、前記復号化手段に、前記暗号化された記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することを特徴とする請求項４または６に記載のデータ記録装置。

【請求項８】　前記記憶手段は、

前記ユーザにより設定され、かつ、入力されたパスワードまたはパスワードおよび補助パスワードを記憶させるか否かを選択可能に設定されていることを特徴とする請求項３乃至７いずれか一項に記載のデータ記録装置。

【請求項９】　前記補助パスワードは当該データ記録装置に関する情報であることを特徴とする請求項６～８のうちいずれか一項に記載のデータ記録装置。

【請求項１０】　前記補助パスワードは複数個設定可能であることを特徴とする請求項６～９のうちいずれか一項に記載のデータ記録装置。

【請求項１１】　前記記憶手段にはハッシュ関数が記憶されていて、

データ書き込み時において、前記制御手段が、

前記暗号化手段に、前記ユーザにより設定され、かつ、入力されたパスワードまたは、前記ユーザにより設定され、かつ、入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、前記記録媒体の認識時に使用されるシステム領域データを暗号化させる処理を実行することを特徴

とする請求項３、５、６、９、１０のうちいずれか一項に記載のデータ記録装置。

【請求項１２】　前記記憶手段にはハッシュ関数が記憶されていて、

データ読み込み時において、前記制御手段が、

前記復号化手段に、ユーザにより設定され、かつ、入力されたパスワードまたは、ユーザにより設定され、かつ、入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、前記暗号化された前記記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することを特徴とする請求項４、５、７、９、１０のうちいずれか一項に記載のデータ記録装置。

【請求項１３】　前記記憶手段は、

前記ハッシュ化された値を記憶させるか否かを選択可能に設定されていることを特徴とする請求項１１または１２に記載のデータ記録装置。

【請求項１４】　前記記録媒体は、リムーバブルであることを特徴とする請求項３～１３のうちいずれか一項に記載のデータ記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はデータ書き込み方法およびデータ読み込み方法と、これらを用いたデータ記録装置に関し、より詳細には、データを効率的に暗号化して記録媒体に記録することが可能なデータ書き込み方法およびデータ読み込み方法と、これらを用いたデータ記録装置に関する。

【０００２】

【従来の技術】

データに機密性を持たせる方法として、暗号化アプリケーションによるデータの暗号化が一般的に用いられている。データの暗号化は、当該データをアプリケーションに搭載されている所定のアルゴリズムによりおこなわれる。このようにして暗号化されたデータは、予め設定されているパスワードを入力し、暗号化アルゴリズムに対応した復号化アルゴリズムにより復号（解読）した後に、データ

が実際に使用可能になる。

近年においては、アプリケーションで行っていたデータの暗号化および復号化処理を記録装置に行わせることを想定した発明が特許文献１に記載されている。

【０００３】

【背景技術】

しかしながら、特許文献１におけるデータ記録装置においては、データを暗号化する際において最も重要であるパスワードについては何ら記載されておらず、パスワードが設定されてなく、単純に平文データ（通常用いられている、暗号化されていないデータをいう）を所定のアルゴリズムで暗号化処理しているものと思われる。

したがって、特許文献１により生成された暗号化データは、暗号化したデータ記録装置と同種類のものを用いれば、誰でも復号（平文化）することができてしまうため、データの機密性が確保できなくなってしまうといった課題や、アプリケーションで平文データを暗号化処理したり、暗号化データを復号化する作業をさせると、パソコンのＣＰＵに負荷をかけてしまうため、暗号化処理や復号化処理を行っている間は、他の作業が円滑に行うことができなくなってしまう等の課題が列挙されていて、本願発明者は、特願２００３－０１４２１９号において、以上の課題を解決したデータ記録装置を提案した。

【０００４】

【特許文献１】

特開平１－２２７２７２号公報

【０００５】

【発明が解決しようとする課題】

ところが、データ記録装置に搭載されているＣＰＵは演算能力が低い場合が多く、記録媒体に記録すべきデータのすべてについて暗号化処理をしようとすると、暗号化処理に時間がかかり、アプリケーションで暗号化処理してから記録媒体にデータを記録する場合よりも時間がかかってしまうことがあるといった新たな課題が見出された。

【０００６】

本発明の目的は、記録媒体に記録すべきデータすべてを暗号化することなく、演算能力の低いＣＰＵであっても簡単には復号されないようにデータを記録することを可能にしたデータ書き込み方法およびデータ読み込み方法と、これらを用いたデータ記録装置を提供することにある。

【０００７】

【課題を解決するための手段】

本発明は、記憶手段と、記録媒体にデータを書き込むデータ書き込み手段と、ユーザにより設定され、かつ、入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化手段とにより構成されるデータ記録装置におけるデータ書き込み方法であって、前記書込み手段が、外部機器に設けられたライトアプリケーションにより構築された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させるステップと、前記暗号化手段が、ユーザにより設定され、かつ、入力されたパスワードに基づいて前記記録媒体の認識時に使用されるシステム領域データの一部又は全てを所定のアルゴリズムで暗号化するステップと、前記記録媒体に前記データを記憶させるステップと、前記データ書込み手段が、該暗号化した記録媒体の認識時に使用されるシステム領域データを前記記録媒体の所定領域に書き込むステップと、前記データ書き込み手段が、前記データを前記記録媒体に書き込むステップとを有することを特徴とするデータ書き込み方法およびこれを用いたデータ記録装置である。

これにより、記録媒体に記録すべきデータのすべてを暗号化処理しなくて済むため、データ記録装置に搭載されている処理能力の低いＣＰＵであっても、データを保護しながらも高速に書き込みすることができる。

【０００８】

また、他の発明は、記憶手段と、記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、ユーザにより設定され、かつ、入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段とにより構成されるデータ記録装置におけるデータ読み込み方法であって、前記読み込み手段が、前記記録媒体の所定領域に格納されている記録媒体の認識時に使用されるシステム領域データにアクセスすると共に、暗号化された記録媒体

の認識時に使用されるシステム領域データを前記記憶手段に記憶させるステップと、前記復号化手段が、ユーザにより設定され、かつ、入力されたパスワードに基づいて、所定のアルゴリズムにより前記記録媒体の認識時に使用されるシステム領域データを復号化するステップとを有することを特徴とするデータ読み込み方法およびこれを用いたデータ記録装置である。

これにより、記録媒体に記録すべきデータのすべてが暗号化処理されていなくても、パスワードを入力しなければ、ファイルシステムデータを正しく参照することができないため、記録媒体に記憶させるすべてのデータが暗号化されていなくても、暗号化処理されたと同程度の機密性を有させることができる。

【０００９】

さらに他の発明は、記憶手段と、記録媒体にデータを書き込むデータ書き込み手段と、記録媒体に書き込まれているデータを読み取るデータ読み込み手段と、ユーザにより設定され、かつ、入力されたパスワードをもとにして、所定のアルゴリズムによりデータを暗号化する暗号化手段と、ユーザにより設定され、かつ、入力されたパスワードをもとにして所定のアルゴリズムにより暗号化されたデータを復号する復号化手段と、各手段の動作を制御する制御手段とにより構成され、データ書き込み時において、前記制御手段が、前記書込み手段に、外部機器に設けられたライトアプリケーションにより構築された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、前記暗号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて前記記録媒体の認識時に使用されるシステム領域データの一部又は全てを所定のアルゴリズムで暗号化させ、前記記憶手段に前記データを記憶させ、前記データ書込み手段に、該暗号化した記録媒体の認識時に使用されるシステム領域データを前記記録媒体の所定領域に書き込ませ、前記データ書き込み手段に、前記データを前記記録媒体に書き込ませる処理を実行し、データ読み込み時において、前記制御手段が、前記読み込み手段に、前記記録媒体の所定領域に格納されている記録媒体の認識時に使用されるシステム領域データにアクセスさせると共に、暗号化された記録媒体の認識時に使用されるシステム領域データを前記記憶手段に記憶させ、前記復号化手段に、ユーザにより設定され、かつ、入力されたパスワードに基づいて、所

定のアルゴリズムにより前記記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することを特徴とするデータ記録装置である。

これにより、記録媒体に記録すべきデータのすべてを暗号化処理しなくて済むため、データ記録装置に搭載されている処理能力の低いＣＰＵであっても、データを保護しながらも高速に書き込みすることができると共に、記録媒体に記録すべきデータのすべてが暗号化処理されていなくても、パスワードを入力しなければ、ファイルシステムデータを正しく参照することができないため、記録媒体に記憶させるすべてのデータが暗号化されていなくても、暗号化処理されたと同程度の機密性を有させることができる。

【００１０】

また、記憶手段には、補助パスワードがあらかじめ記憶されていて、前記制御手段は、ユーザにより設定され、かつ、入力されたパスワードに、前記補助パスワードを付加した後に、前記暗号化手段に前記記録媒体の認識時に使用されるシステム領域データを暗号化させる処理を実行することも可能である。

これにより、暗号化したファイルシステムデータを復号処理する際における属性を付加させることが可能になる。またさらには、暗号化したファイルシステムデータを復号化処理する際におけるデータの機密性を向上させることが可能になる。

さらに、前記記憶手段には、補助パスワードがあらかじめ記憶されていて、前記制御手段は、ユーザにより設定され、かつ、入力されたパスワードに前記補助パスワードを付加した後に、前記復号化手段に、前記暗号化された記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することも可能である。

これによれば、属性を有する暗号化されたファイルシステムデータを復号処理することが可能になる。

【００１１】

また、前記記憶手段は、前記ユーザにより設定され、かつ、入力されたパスワードまたはパスワードおよび補助パスワードを記憶させるか否かを選択可能に設定されていることが好ましい。

これによれば、いちいちパスワードを設定しなくても済み、限られたワークグループ内での使用においては、グループ内での記憶装置の設定を一致させておけば、そのワークグループ内でしかデータを復号することができなくすることができるので、使い勝手が向上する。

【００１２】

さらにまた、前記補助パスワードは当該データ記録装置に関する情報であることが好ましい。

これにより、ユーザが設定した任意の文字列からなるパスワードに補助パスワードを組み合わせて鍵を形成し、暗号化手段により暗号化がなされることになるため、たとえ、ユーザが設定したパスワードを入手したとしても、暗号化したファイルシステムを復号処理させることができなくなるため好適である。

また、補助パスワードは複数設定することが可能であることが好ましい。

これにより、暗号化処理したデータの機密性をさらに向上させることが可能になる。

【００１３】

さらにまた、前記記憶手段にはハッシュ関数が記憶されていて、データ書き込み時において、前記制御手段が、前記暗号化手段に、前記ユーザにより設定され、かつ、入力されたパスワードまたは、前記ユーザにより設定され、かつ、入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、前記記録媒体の認識時に使用されるシステム領域データを暗号化させる処理を実行することが好ましい。

これによれば、ユーザが設定したパスワードの長短によるパスワードの強度のばらつきをなくし、均一のレベルにすることが可能になる。また、暗号化する際に用いる鍵の長さを一定にすることができるので、処理が容易に行うことができる。

また、前記記憶手段にはハッシュ関数が記憶されていて、データ読み込み時において、前記制御手段が、前記復号化手段に、ユーザにより設定され、かつ、入力されたパスワードまたは、ユーザにより設定され、かつ、入力されたパスワードおよび前記補助パスワードを、当該ハッシュ関数によりハッシュ化した後に、

前記暗号化された前記記録媒体の認識時に使用されるシステム領域データを復号化させる処理を実行することが好ましい。

これによれば、ユーザが設定したパスワードの長短等によるパスワードの強度のばらつきをなくし、均一のレベルにすることが可能になる。また、暗号化や復号化する際に用いる鍵の長さを一定にすることができるので、処理を容易に行うことができる。

【００１４】

さらに、前記記憶手段は、前記ハッシュ化された値を記憶させるか否かを選択可能に設定されていることが好ましい。

これにより、いちいちパスワードの設定が不要になるため、ある一定の範囲内（限られたユーザどうしの間）のみの記録装置の使用である場合には、記録装置の設定を一致させておけば、限られたユーザどうし間でのみ使用することが可能になる。

【００１５】

また、前記記録媒体は、リムーバブルであることが好ましい。

これによれば、データの供給先のデータ記録装置の規格が共通していれば、該データ記録装置の設定を供給元のデータ記録装置の設定に合わせることにより、ファイルシステムデータを暗号化処理した記録装置以外の記録装置においてもデータを復号することができるため、暗号化データの使用が認められているユーザ間においては暗号化処理した記録媒体の共有が容易になり、利便性が向上する。

【００１６】

【発明の実施の形態】

以下、本発明に係るデータ記録装置の好適な実施の形態を添付図面に基づいて詳細に説明する。

なお本発明は、本実施の形態に限定されるものではなく、発明の要旨を変更しない範囲において、各種の改変がなされても本発明の技術的範囲に属するのは言うまでもない。

【００１７】

（第１の実施の形態）

まず、本実施の形態におけるデータ記録装置の概要について図１を用いて説明する。本実施の形態においては、データ記録装置として光ディスク装置を用いることにする。図１は、暗号化機能を有する光ディスク装置の構成を示す説明図である。

本発明に係る暗号化機能を有する光ディスク装置１０は、パーソナルコンピュータ等の外部機器４０に設置され、外部機器４０から当該光ディスク装置１０を操作可能にする操作用入力手段であるアプリケーション４２と、アプリケーション４２の一機能として設けられ、記録媒体（光ディスク）に記録されているデータ情報を示すファイルシステムデータ（記録媒体の認識時に使用されるシステム領域データ）を構築するファイルシステムデータ構築手段４４と、パーソナルコンピュータ等の外部機器４０から送られてくるデータを一時記憶する記憶手段１４と、記憶手段１４に一時記憶されたデータを記録媒体である光ディスク３０に書き込むデータ書き込み手段１６と、ユーザにより設定され、アプリケーション４２から入力されたパスワードを用いて、ファイルシステムデータを所定の方法で暗号化する暗号化手段１８と、光ディスク３０に記録された暗号化データを読み取るデータ読み込み手段２０と、アプリケーション４２から入力されたパスワードを用いて、暗号化されたファイルシステムデータを復号する復号化手段２２と、これらの動作を制御する制御手段１２とにより構成されている。

【００１８】

本実施の形態においては、光ディスク装置１０における暗号化手段１８と、復号化手段２２は、それぞれ別体であるとしているが、光ディスク装置１０に内蔵されているＣＰＵ等の制御手段１２がこれらを統括して実行処理する形態であっても良いのはもちろんである。

また、データ書き込み手段１６とデータ読み込み手段２０とについては、光ピックアップ（図示せず）にひとまとめにしてしまうのも、もちろん可能である。

【００１９】

アプリケーション４２は、パーソナルコンピュータ等の外部機器４０の図示しない記憶手段にインストールされていて、外部機器４０でアプリケーション４２を起動し、アプリケーション４２を操作することにより、光ディスク装置１０の

制御手段１２に各種のコマンドを送信して光ディスク装置１０の動作を制御することが可能である。

アプリケーション４２から光ディスク３０へデータを記録させるコマンドを光ディスク装置１０に送信すると、制御手段１２は、光ディスク装置１０の記憶手段１４にデータを一時記憶させた後、データ書き込み手段１６が記憶手段１４に記憶されたデータを光ディスク３０に書き込み、必要に応じて光ディスク３０そのものを暗号化処理する。

また、アプリケーション４２が記録媒体の認識時に使用されるシステム領域データの一例としてのファイルシステムを構築する機能であるファイルシステム構築手段４４を有する。

【００２０】

ファイルシステムデータ構築手段４４は、光ディスク３０に書き込むデータのファイルを管理するための制御データであるファイルシステムデータを構築するものである。

ファイルシステムデータについて図２に基づいて説明する。図２はファイルシステムデータの構造を示す説明図である。

光ディスクの分野でいうファイルシステムデータは、ＩＳＯ９６６０の規格によれば、データエリア４の先頭から２ｋＢづつのＬＢＮ（Logical Block Number）が０から１５まで割り振られているが、ＬＢＮ１６からは、ファイルシステムデータ６が記述される。

【００２１】

ファイルシステムデータ６には、ＰＶＤ（Primary Volume Descriptor）７、パステーブル８、ルートディレクトリ９、およびルートディレクトリの下層に位置する複数のチャイルドディレクトリ５を含んでいる。

ＰＶＤ７には、ファイルフォーマットの識別、ボリュームの大きさ、パステーブル８の大きさやアドレス等の種々の情報が記録されている。

パステーブル８には、階層構造を持ったチャイルドディレクトリ５のそれぞれのアドレスが記録されている。パステーブル８を読み取ることで、複数のチャイルドディレクトリ５のそれぞれのアドレスその他の情報を得ることができる。

なお、ファイルシステムデータの例としては、ＩＳＯ９６６０の規格に準拠したものについて限定されるものではない。他の規格ではファイルシステムデータの存在する場所も異なってくる。

【００２２】

本発明に係る光ディスク装置１０においては、データ書き込み手段１６がデータを光ディスク３０に書き込む前に、ファイルシステムデータ構築手段４４が、書き込むべきデータを階層構造に構築し、各ファイルの開始アドレスやデータ長をもとにファイルシステムデータ６を作成してデータエリア４に記録する。

なお、本実施形態では、ファイルシステムデータは、暗号化手段１８によって、ユーザにより設定され、アプリケーション４２から入力されたパスワードに基づいて、所定の方法（後述する）により暗号化処理された後に、光ディスク３０に記録されることになる。

【００２３】

このように、ファイルシステムデータを暗号化して記録媒体に書き込むことにより、かかる記録媒体が装着された読み出し機器側では、書き込まれているデータのファイルフォーマットの種類や各ファイルの開始アドレス等も全くわからなくなる。このため、ファイルシステムデータのみを暗号化しておけば、記録媒体の内容すらわからなくなっているのでデータそのものが暗号化されていなくても、記録媒体としては良好な秘密性を保持しつつ、暗号化処理に要する時間を短縮できる。

【００２４】

暗号化手段１８は、ファイルシステムデータを暗号化処理するものである。暗号化処理手段１８は、ユーザが設定し、アプリケーション４２から入力されたパスワードに基づいて所定のアルゴリズムを実行する。暗号化手段１８は、ユーザが設定したパスワードの他に、補助パスワードを付加させることも可能であり、補助パスワードの付加により、より高度な暗号化処理が可能になる。

補助パスワードは、工場出荷時において光ディスク装置１０に附されているシリアルナンバーや、機種名あるいは暗号化データの使用が許可されているグループ名等を設定し、あらかじめ記憶手段１４に記憶させておくと共に、アプリケー

ション４２の選択ボタンに関連付けしておけば好適である。また、複数の補助パスワードを設定することも可能であり、ある補助パスワードは、工場出荷時に設定されていて、他の補助パスワードは、ユーザにより設定可能にしておけばさらに好適である。

【００２５】

これらの複数の補助パスワードにより、暗号化処理は、ユーザが設定した任意の文字列からなるパスワードに補助パスワードを組み合わせて鍵を形成し、暗号化手段１８によりなされることになるため、ユーザが設定したパスワードを入手したのみでは、暗号化データを復号処理させることができなくなり好適である。なお、補助パスワードを用いずにユーザが設定したパスワードのみで鍵を形成する形態としてもよいのはもちろんである。

このようにユーザの設定したパスワードに補助パスワードを付加させることが可能になっているので、ユーザにより設定されるパスワードはブランク（空白）のパスワードとし、補助パスワードのみの文字列で鍵を形成させることも十分に可能である。

【００２６】

暗号化手段１８に組み込まれているアルゴリズムには様々な規格が存在しているが、本実施の形態においては、ユーザにより設定された任意の文字列またはユーザにより設定された任意の文字列に、補助パスワードを加えた文字列を鍵とした暗号化処理方式が用いられている。このような暗号化方式として、例えば、秘密鍵暗号であるＤＥＳ方式等が挙げられるが、この暗号化方式に限定されるものではない。

なお、復号化手段２２は、少なくとも暗号化手段１８に対応したアルゴリズムが組み込まれているのは言うまでもない。

【００２７】

なお、ファイルシステムデータを暗号化する際においては、ファイルシステムデータ全部を暗号化するのではなく、ファイルシステムデータの一部のみを暗号化する方法としてもよいのはもちろんである。

例えば、ＰＶＤ７のみを暗号化しても、光ディスク装置１０が光ディスク３０に

記録されているファイルフォーマットを識別することができなくなるので、暗号化の効果を十分得ることができる。

【００２８】

第１の実施の形態における光ディスク装置のデータ処理工程について説明する。図３は、第１の実施の形態におけるデータ処理工程の概略を示す説明図である。

パーソナルコンピュータ等の外部機器４０からアプリケーション４２を介して、ユーザが暗号化処理を選択した場合には、光ディスク装置１０に暗号化処理コマンドが送信される（Ｓ１０１）。ユーザは引き続きアプリケーション４２上で暗号化処理をしたデータの復号化処理の態様を選択する（Ｓ１０２）。続いてデータを暗号化処理する際に必要なパスワードを入力する（Ｓ１０３）。

【００２９】

パスワードが入力されたら、制御手段１２が、記憶手段１４に記憶される復号化処理の態様を見分けるための補助パスワードをパスワードに付加する（Ｓ１０４）。続いてライティングソフトが具備するファイルシステムデータ構築手段４４が光ディスクのファイルシステムデータを構築する（Ｓ１０５）。

次にパーソナルコンピュータ等の外部機器４０からアプリケーション４２を介して、ファイルシステムデータを含むデータを光ディスク装置１０の記憶手段１４が受信し（Ｓ１０６）、受信したデータが記憶手段１４に一時保管される（Ｓ１０７）。

その後、アプリケーション４２を介してユーザが光ディスクの暗号化処理をするか否かを選択する（Ｓ１０８）。ここで、光ディスク３０の暗号化処理が選択されなかった場合には、通常の手順によって光ディスク３０にデータが書き込まれる（Ｎ－１）ことにより、光ディスク３０へのデータの書き込みが完了する。反面、光ディスク３０の暗号化処理が選択された場合は、暗号化手段１８がパスワードと補助パスワードを合わせた文字列を鍵としてファイルシステムデータの一部を暗号化処理し（Ｓ１０９）、暗号化されたファイルシステムを含むデータがそれぞれ光ディスク３０の所定の領域に、データ書き込み手段１６によって記録される（Ｓ１１０）。

【００３０】

光ディスク３０を暗号化処理した場合、光ディスク３０に記録されたデータを読み取る際は復号処理が必要になる。復号処理についての手順を説明する。まず、光ディスク３０を光ディスク装置１０にセットし（Ｓ１１１）、データ読み込み手段２０が光ディスク３０に書きこまれている暗号化されているファイルシステムデータにアクセスし、暗号化されているファイルシステムデータを記憶手段１４に記憶させる（Ｓ１１２）。続いて、アプリケーション４２上から復号化の態様を選択し（Ｓ１１３）、光ディスク３０を暗号化処理する際に設定したパスワードと、補助パスワードをそれぞれ入力する（Ｓ１１４、Ｓ１１５）。

【００３１】

制御手段１２は、記憶手段１４に記憶されている光ディスク３０に記録されていた、暗号化処理されたファイルシステムデータをデータ読み込み手段２０にアクセスさせ、暗号化ファイルシステムデータを復号化手段２２に送信し、復号化手段２２がアプリケーション４２を介してユーザにより設定されて入力されたパスワードに、同じくアプリケーション４２で選択された復号化態様に関連付けられている補助パスワードを付加した文字列より成る鍵を用いて復号処理を行う（Ｓ１１６）。パスワードが正しければ暗号化されたファイルシステムデータは通常のファイルシステムデータに変換され、制御手段１２により光ディスク３０内のデータ記録構造が把握され、光ディスク３０に記録されているデータにアクセスして、所望のデータを利用する（Ｓ１１７）ことが可能になる。

反面、入力されたパスワードが正しくなければ、暗号化処理されたファイルシステムデータは正しく変換されないため、制御手段１２がファイルシステムデータを正しく認識することができないので、光ディスク３０を認識することさえできなくなる。

【００３２】

（第２の実施の形態）

第１の実施の形態においては、ユーザが設定したパスワードまたは、ユーザが設定したパスワードに復号化の態様に関連付けられた補助パスワードから成る文字列を鍵として、ファイルシステムデータを暗号化処理および復号化処理を行う

形態であるが、本実施の形態においては、第１の実施の形態における光ディスク装置１０にパスワード変換手段２６を追加し、パスワードまたは、パスワードおよび補助パスワードから成る文字列を所定の関数により数値変換し、その数値を鍵としてファイルシステムデータを暗号化処理および復号化処理を行うことを特徴としている。

【００３３】

図４は第２の実施の形態における光ディスク装置１０の内部構成を示す説明図である。なお、本実施の形態において、第１の実施の形態と共通する構成要素については、第１の実施の形態と同じ符号を附すことにより、それらの要素についての詳細な説明は省略する。

パスワード変換手段２６は、ユーザにより設定されたパスワードまたは、ユーザにより設定されたパスワードおよび復号化形態に関連付けされている補助パスワードから成る文字列を数値化するための手段である。任意の文字列を数値化する手段としては様々な形式のものが提供されているが、本実施の形態においては、ハッシュ関数を用いることにしている。ハッシュ関数は、一方向関数であり、ハッシュ関数により得られた数値から元のパスワードを推測することは事実上不可能であるので、データ保護の安全性を向上させることができ、好適である。

【００３４】

第２の実施の形態における光ディスク装置のデータ処理工程について説明する。図５は、第２の実施の形態におけるデータ処理工程の概略を示す説明図である。

アプリケーション４２を介して、ユーザが光ディスク装置１０に光ディスク３０を暗号化処理させる選択をした場合、光ディスク装置１０に暗号化処理コマンドが送信される（Ｓ２０１）。ユーザは引き続き、アプリケーション４２上で暗号化処理をしたデータの復号化処理の態様を選択する（Ｓ２０２）。続いてデータを暗号化処理する際に必要なパスワードを入力する（Ｓ２０３）。パスワードが入力されたら、制御手段１２が、記憶手段１４に記憶される復号化処理の態様を見分けるための補助パスワードをパスワードに付加する（Ｓ２０４）。

【００３５】

次に、パスワード変換手段２６が、パスワードと補助パスワードを複合したパスワードを数値に変換（ハッシュ化）し（Ｓ２０５）、ファイルシステムデータ構築手段４４が光ディスクのファイルシステムデータを構築する（Ｓ２０６）。
続いて、パーソナルコンピュータ等の外部機器４０から光ディスク３０に記録すべきデータ（ファイルシステムデータを含む）を光ディスク装置１０の記憶手段１４が受信する（Ｓ２０７）。記憶手段１４は送られてきたデータを一時保管する（Ｓ２０８）。
その後、アプリケーション４２を介してユーザが光ディスク３０を暗号化処理するか否かを選択する（Ｓ２０９）。ここで、暗号化処理が選択されなかった場合には、通常の手順によって光ディスク３０にデータが書き込まれる（Ｎ－１）ことにより、光ディスク３０へのデータの書き込む処理が完了する。反面、暗号化処理が選択された場合には、暗号化手段１８が、パスワードをハッシュ化して得られた数値を鍵として、記憶手段１４に記憶させたファイルシステムデータを所定の方式により暗号化処理を行い（Ｓ２１０）、データ書き込み手段１６が、暗号化処理されたファイルシステムを含むデータをそれぞれ光ディスク３０の所定の領域に記録する（Ｓ２１１）。

【００３６】

暗号化されたデータを復号する際は、光ディスク３０を光ディスク装置１０にセットし（Ｓ２１２）、データ読み込み手段２０が暗号化されたファイルシステムデータにアクセスして記憶手段１４に暗号化されたファイルシステムを一時記憶させる（Ｓ２１３）。ユーザがアプリケーション４２上から復号化の態様を選択し（Ｓ２１４）、ファイルシステムデータを暗号化処理した際に設定したパスワードを入力する（Ｓ２１５）。制御手段１２は、ユーザにより入力されたパスワードに復号化の態様に関連付けられている補助パスワードを付加し（Ｓ２１６）た後、所定の関数に基づいて数値に変換（ハッシュ化）する（Ｓ２１７）。復号化手段２２は、パスワードを変換して得られた数値（ハッシュ値）を鍵としてファイルシステムデータを復号処理する（Ｓ２１８）。

【００３７】

アプリケーション４２から入力されたパスワードが正しければ、パスワード変換

手段２６により変換されて得られる数値（鍵）が一致するので、ファイルシステムデータは、復号化手段２２により正しく復号される。これにより制御手段１２が光ディスク３０のファイル構造を認識することができるため、光ディスク３０からデータを取り出して所望のデータを利用する（Ｓ２１９）ことが可能になる。

【００３８】

なお、ハッシュ値を記憶手段１４に記憶させておけば、データ処理のたびにパスワードを設定する必要を無くすことができる。このようにパスワードを記憶手段１４に記憶させる形態は、限られたユーザのみが光ディスク装置にアクセスできる環境においては特に好適である。

【００３９】

以上、実施の形態に基いて本発明に係るデータ記録装置について詳細に説明してきたが、本発明はこれに限定されるものではない。したがって、本発明の要旨を変更しない範囲において本実施の形態について各種の改変がなされたとしても、本発明の技術範囲に属することは言うまでもない。

例えば、暗号化する記憶媒体の認識時に使用されるシステム領域のデータとして、ファイルシステムデータの他に、ＴＯＣ（Table of Contents）やＰＭＡ（Program Memory Area）を暗号化する方法も考えられる。

また、暗号化および復号化形態の態様は、すべて光ディスク装置で暗号化、復号化処理する態様のみを想定しているが、データの暗号化および／または復号化を暗号化アプリケーションの態様に対応させるようにしてもよいのはもちろんである。これによれば、他の暗号化アプリケーションで暗号化等したデータを、実際に暗号化処理したアプリケーションなしでも復号処理等をすることができる。

【００４０】

さらに、本実施の形態においては、暗号化方式に秘密鍵暗号方式を採用しているが、公開鍵暗号方式を用いてもよいのはもちろんである。

さらにまた、補助パスワードは、必ずしも光ディスク装置に関する情報でなくても良く、ユーザにより任意に設定された文字列を記憶手段に記憶させる形態としても良い。

【００４１】

また、操作用入力手段は、外部機器に設置したアプリケーションに限られることはなく、データ記録装置の本体に取り付けたものであってもよいのはもちろんである。

さらに、記録媒体は、固定式、リムーバブル式のいずれでもよく、光ディスクに限定されずに、固定ディスクや光磁気ディスクおよび磁気ディスク等を用いることももちろん可能である。

【００４２】

【発明の効果】

以上のことから、本発明におけるデータ記録装置を用いることにより以下に示す効果がある。

すなわち、本発明においては、光ディスク情報であるファイルシステムデータのみを暗号化処理することにより、記録媒体に記録すべきデータのすべてを暗号化処理しなくて済むため、データ記録装置に搭載されている処理能力の低いＣＰＵであっても、データを保護しながらも高速に書き込みすることができる。

また、記録媒体に記録すべきデータのすべてが暗号化処理されていなくても、パスワードを入力しなければ、ファイルシステムデータを正しく参照することができないため、記録媒体に記憶させるすべてのデータが暗号化されていなくても、暗号化処理されたと同程度の機密性を有させることができる。

さらに、記録装置自体にファイルシステムデータを暗号処理するアルゴリズムと復号処理するアルゴリズムが組み込まれているので、データ記録装置に搭載されている処理能力の低いＣＰＵであっても、データを保護しながらも高速に書き込みすることができると共に、記録媒体に記録すべきデータのすべてが暗号化処理されていなくても、パスワードを入力しなければ、ファイルシステムデータを正しく参照することができないため、記録媒体に記憶させるすべてのデータが暗号化されていなくても、暗号化処理されたと同程度の機密性を有させることができる。

【００４３】

さらにまた、記憶手段には、ユーザにより設定されたパスワードに追加する補

助パスワードがあらかじめ記憶されていることにより、暗号化したファイルシステムデータを復号化処理する際の属性を付加させることが可能になる。またさらには、暗号化したファイルシステムデータを復号化処理する際におけるファイルシステムデータの機密性を向上させることが可能になる。

また、ユーザが設定したパスワードと、復号化処理の属性に関連付けされた補助パスワードを記憶手段に記憶させるか否かを選択可能にしたことにより、たとえば、オフィスの同一グループ内での使用のように、何回も同じ条件で暗号化処理および復号化処理をする場合において、その都度パスワードの設定をする必要がなくなるため、ファイルシステムデータの機密性を維持しながらも記録装置の使用方法を簡素化することができる。

さらにまた、補助パスワードをデータ記録装置に関する情報とすることにより、記録媒体を実際に暗号化処理させたユーザであれば補助パスワードによる属性を分かりやすくすることができる。

【００４４】

さらに、パスワードをハッシュ関数によりハッシュ化してから暗号化または復号化処理をすることにより、ユーザが設定したパスワードの長短によるパスワードの強度を均一のレベルにすることが可能になる。

また、パスワードまたは複合パスワードのハッシュ値を記憶手段に記憶させることが可能に設定されているため、たとえば、オフィスの同一グループ内での使用のように、何回も同じ条件で暗号化処理および復号化処理をする場合において、その都度パスワードの設定をする必要がなくなるため、ファイルシステムデータの機密性を維持しながらも記録装置の使用方法を簡素化することができる。

【００４５】

さらに、前記記録媒体を、リムーバブルとしたことにより、データ記録装置が共通していれば、該データ記録装置の設定を供給元のデータ記録装置の設定に合わせれば、暗号化したファイルシステムデータを復号することができるため、暗号化した記録媒体の共有が容易になり、利便性が向上する等といった著効を奏する。

【図面の簡単な説明】

【図１】　第１の実施の形態における光ディスク装置の構成を示す説明図である。

【図２】　ファイルシステムデータの構造を示す説明図である。

【図３】　第１の実施の形態におけるデータ処理工程の概略を示す説明図である。

【図４】　第２の実施の形態における光ディスク装置の構成を示す説明図である。

【図５】　第２の実施の形態におけるデータ処理工程の概略を示す説明図である。

【符号の説明】

１０　光ディスク装置

１２　制御手段

１４　記憶手段

１６　データ書き込み手段

１８　暗号化手段

２０　データ読み込み手段

２２　復号化手段

２６　パスワード変換手段

３０　光ディスク

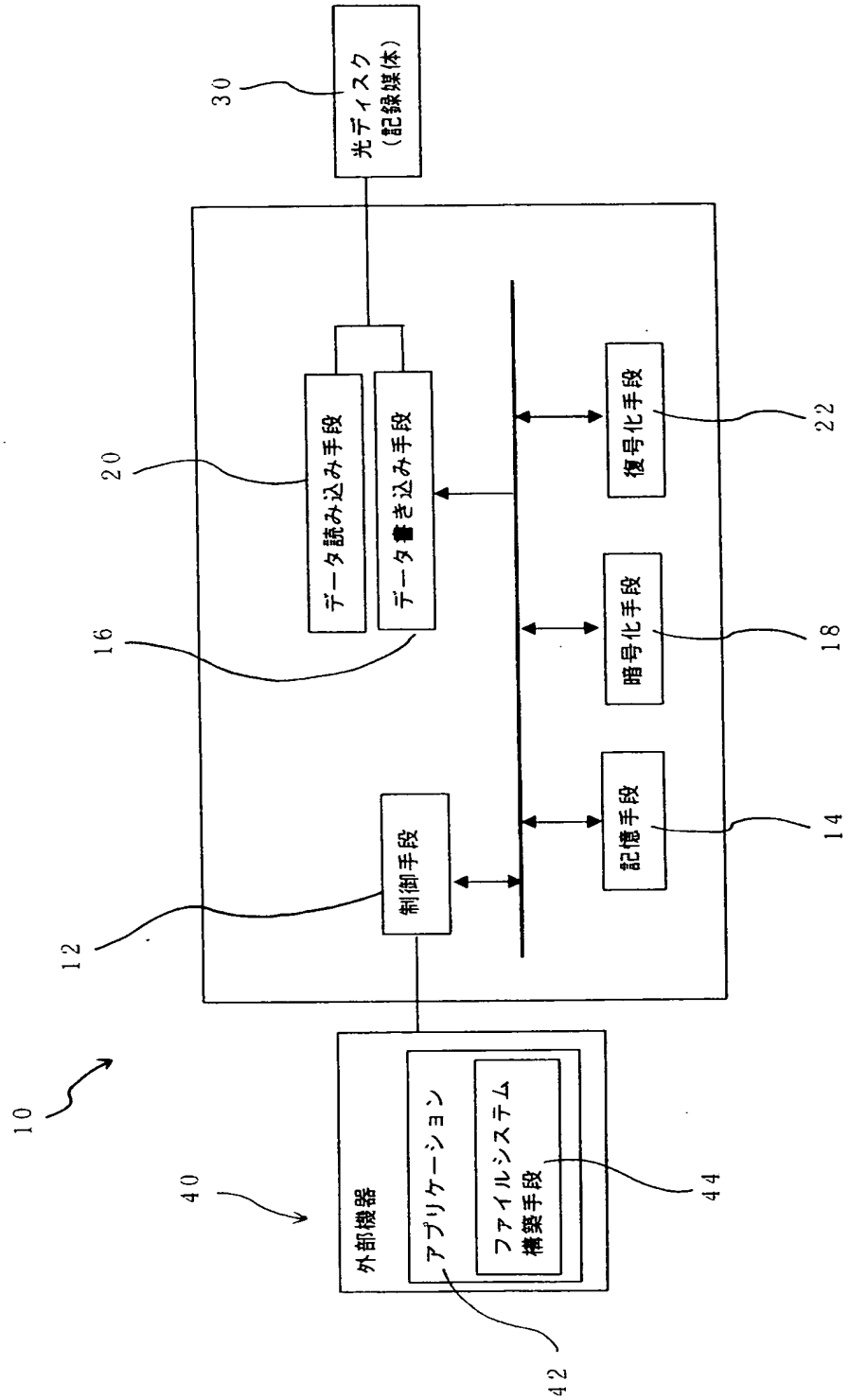
４０　外部機器

４２　アプリケーション

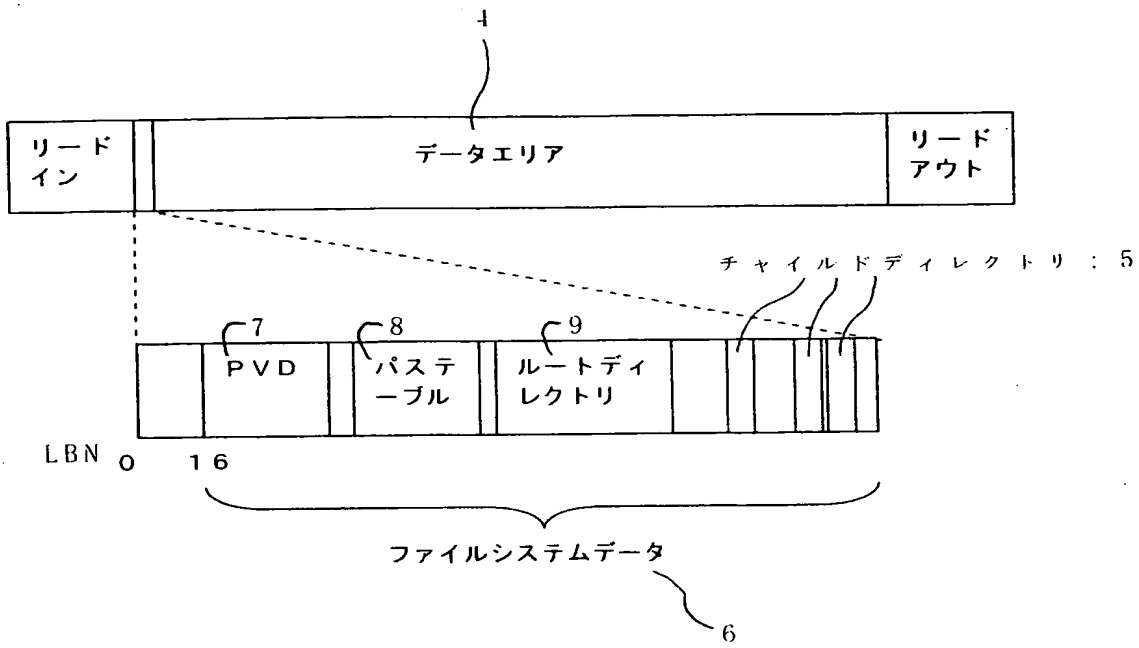
４４　ファイルシステムデータ構築手段

【書類名】　　図面

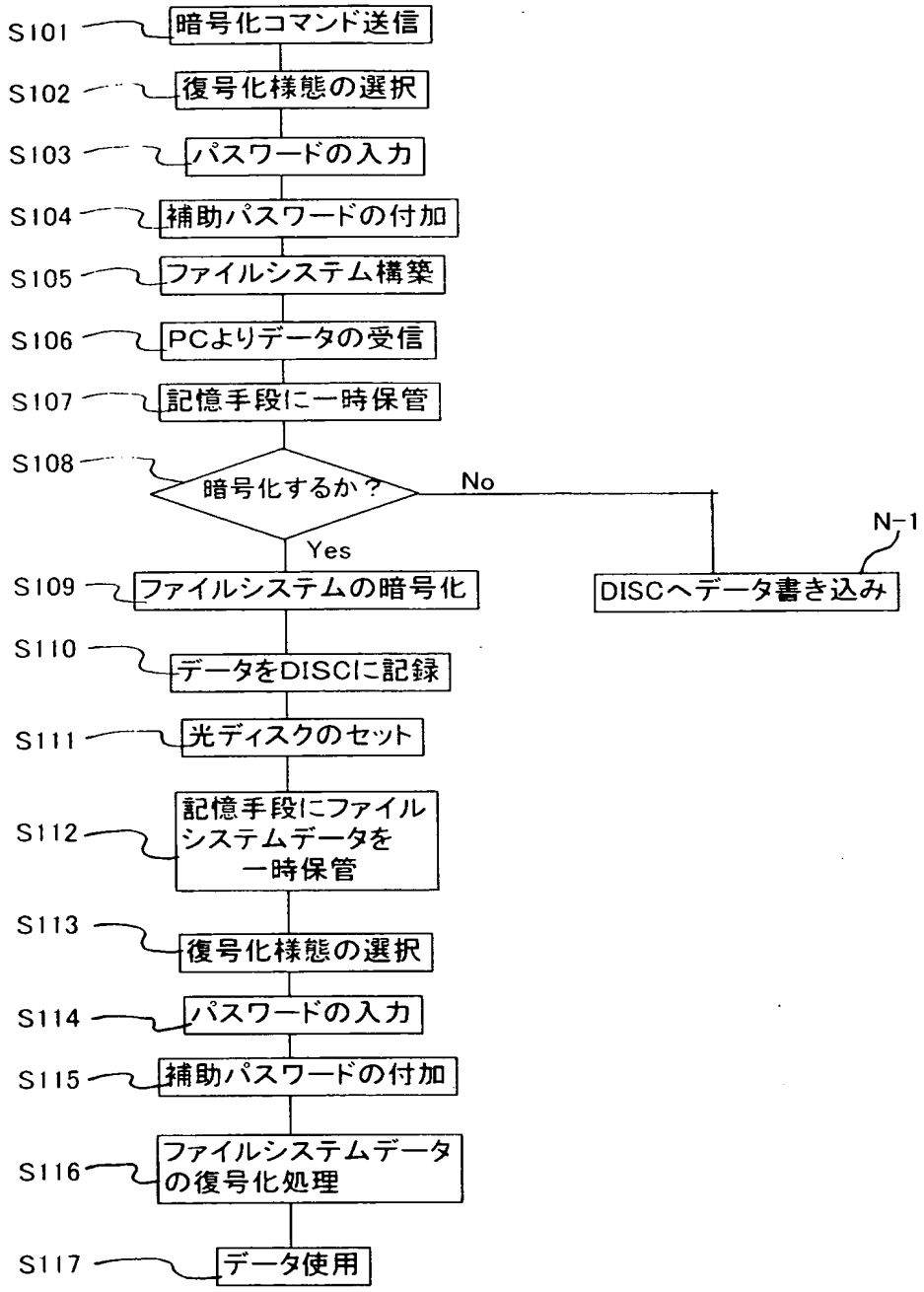
【図１】


光ディスク
（記録媒体）
30
データ読み込み手段
データ書き込み手段
20
16
復号化手段
22
暗号化手段
18
記憶手段
14
制御手段
12
10
外部機器
アプリケーション
ファイルシステム
構築手段
40
42
44

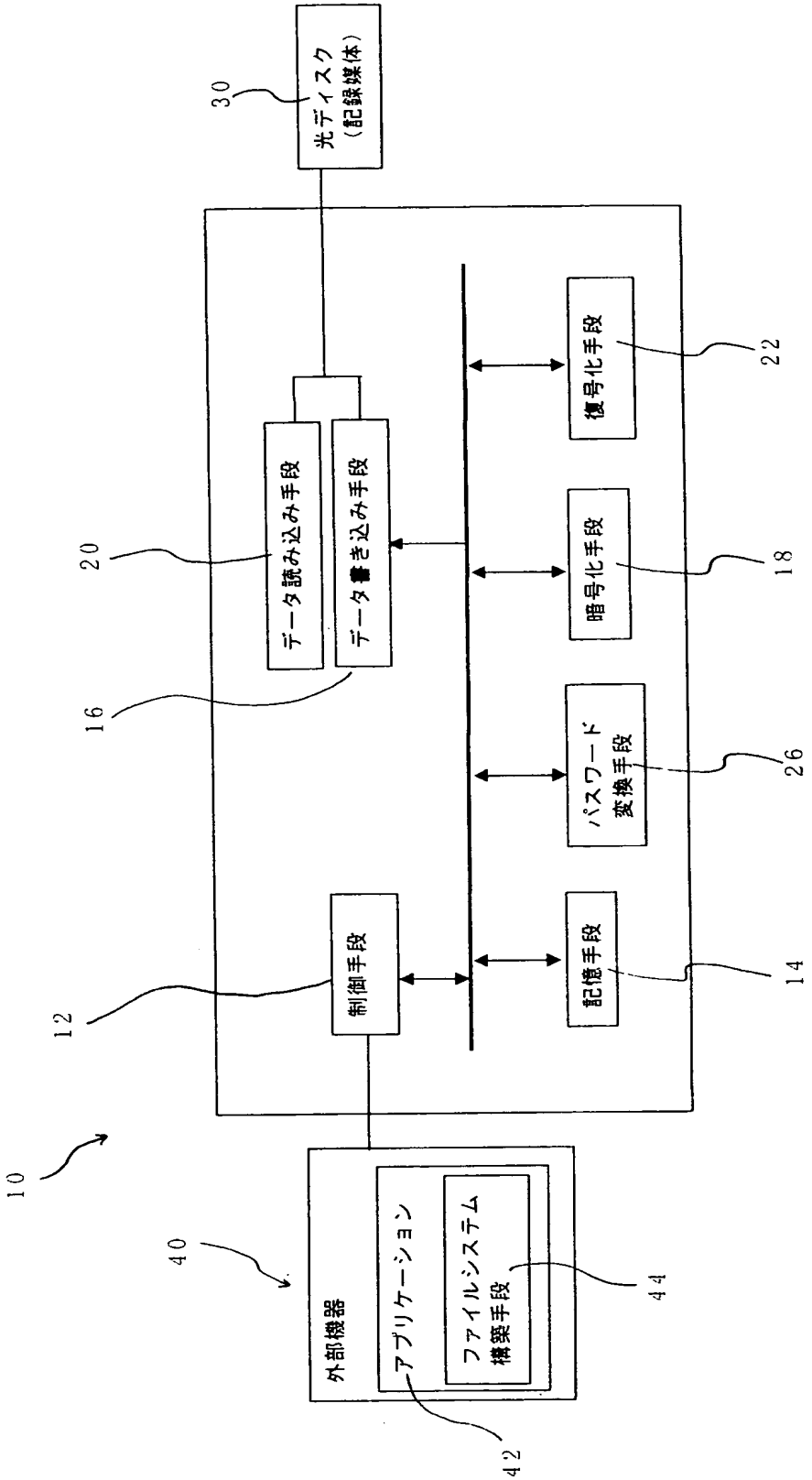
【図２】


4
リード
イン
データエリア
リード
アウト
チャイルドディレクトリ：5
7
8
9
PVD
パステ
ーブル
ルートディ
レクトリ
LBN 0
16
ファイルシステムデータ
6

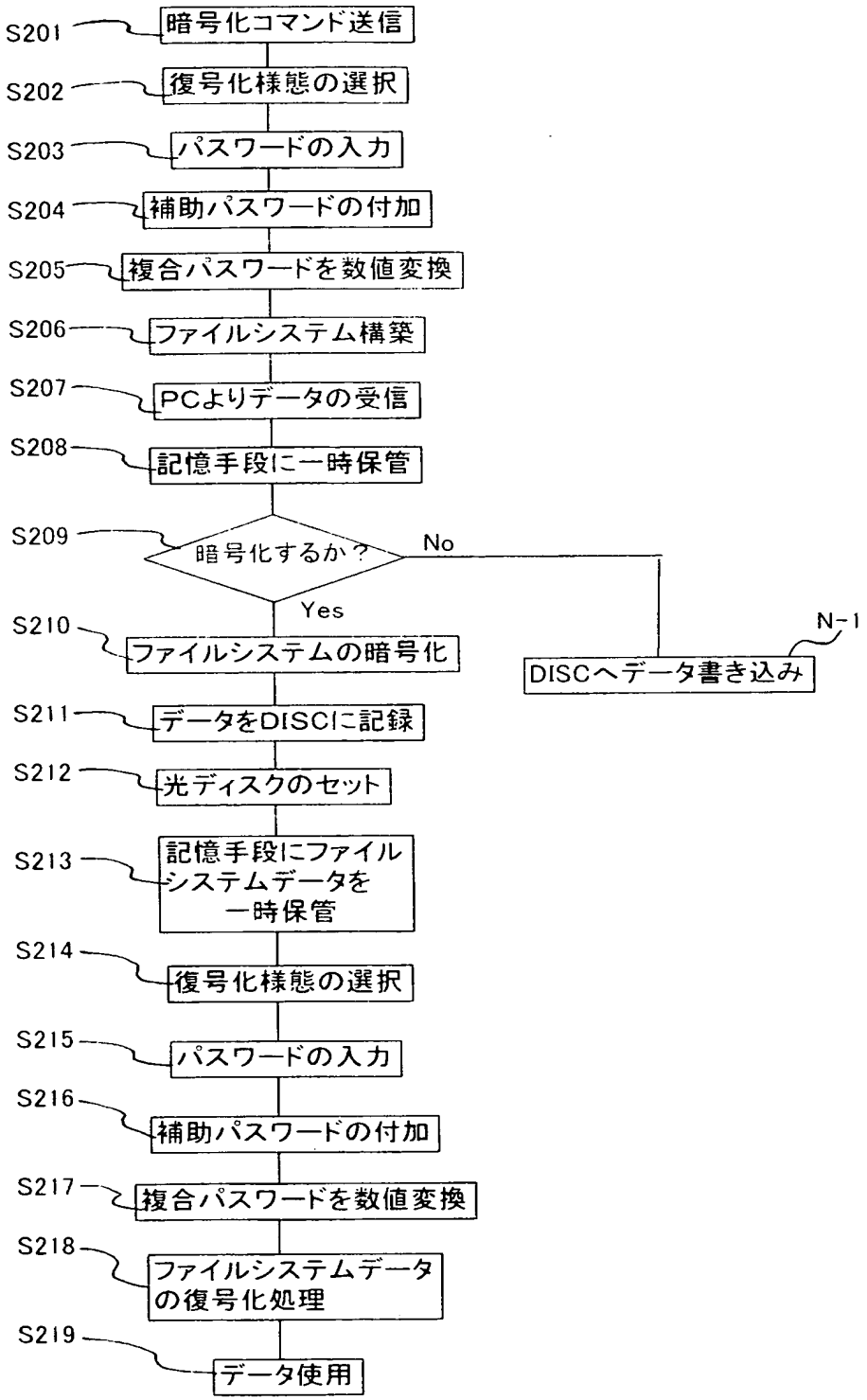
【図３】


S101
暗号化コマンド送信
S102
復号化様態の選択
S103
パスワードの入力
S104
補助パスワードの付加
S105
ファイルシステム構築
S106
PCよりデータの受信
S107
記憶手段に一時保管
S108
暗号化するか？
No
Yes
N-1
DISCへデータ書き込み
S109
ファイルシステムの暗号化
S110
データをDISCに記録
S111
光ディスクのセット
S112
記憶手段にファイルシステムデータを一時保管
S113
復号化様態の選択
S114
パスワードの入力
S115
補助パスワードの付加
S116
ファイルシステムデータの復号化処理
S117
データ使用

【図４】


光ディスク
（記録媒体）
30
データ読み込み手段
データ書き込み手段
20
16
復号化手段
22
暗号化手段
18
パスワード
変換手段
26
制御手段
12
記憶手段
14
10
外部機器
40
アプリケーション
42
ファイルシステム
構築手段
44

【図５】


S201
暗号化コマンド送信
S202
復号化様態の選択
S203
パスワードの入力
S204
補助パスワードの付加
S205
複合パスワードを数値変換
S206
ファイルシステム構築
S207
PCよりデータの受信
S208
記憶手段に一時保管
S209
暗号化するか？
No
Yes
S210
ファイルシステムの暗号化
N-1
DISCへデータ書き込み
S211
データをDISCに記録
S212
光ディスクのセット
S213
記憶手段にファイルシステムデータを一時保管
S214
復号化様態の選択
S215
パスワードの入力
S216
補助パスワードの付加
S217
複合パスワードを数値変換
S218
ファイルシステムデータの復号化処理
S219
データ使用

【書類名】　　要約書

【要約】

【課題】　記録装置のＣＰＵで効率的にデータの暗号化が可能なデータ記録方法とデータ記録装置を提供する。

【解決手段】　記憶手段１４と、記録媒体にデータを書込むデータ書込手段１６と、ユーザにより設定されたパスワードをもとに、所定のアルゴリズムでデータを暗号化する暗号化手段１８とで構成されるデータ記録装置１０のデータ書込方法であって、書込手段１６が、ファイルシステム領域データ（以下、ＦＳＤ）を記録手段１４に記録させ、暗号化手段１８が、ユーザにより設定されたパスワードに基づいてＦＳＤの一部又は全てを所定のアルゴリズムで暗号化し、データを記録媒体に記録させるステップと、データ書込手段１６が、暗号化したＦＳＤを記録媒体の所定領域に書き込ませ、データ書込手段１６が、データを記録媒体に書き込ませるステップを有することを特徴とするデータ書き込み方法である。

【選択図】　　図３

特願２００３－１１７３８３

出　願　人　履　歴　情　報

識別番号　［０００１０６９４４］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　長野県小県郡丸子町大字上丸子１０７８
氏　名　シナノケンシ株式会社